Contents

Certificate iii

Declaration by the Candidate v

Copyright Transfer Certificate vii

Acknowledgements ix

Contents xiii

List of Figures xvii

List of Tables xix

Abbreviations xxi

Symbols xxv

Preface xxvii

1 Introduction 1

1.1 Need of Safety Analysis for Safety Critical Systems (SCSs) 7
1.2 History of Safety 9
1.3 Motivation and Objectives of Research 10
1.4 Scope of Research 12
1.5 Thesis Outline 12

2 Preliminaries 17

2.1 Dependability 18

2.1.1 The Threats: Faults, Errors, and Failures 20
2.1.2 The Attributes of Dependability 22
2.1.3 The Means to Attain Dependability 22
2.2 Classification of Computer Based System 23
2.3 Basic Dependability Mathematics 24
2.3.1 Concepts of Probability Theory 24
2.3.2 Time to Failure, Reliability, Hazard rate and their relations . 27
2.3.3 Probability Distributions Used in Safety Studies 29
2.4 Dependability Attribute Prediction Metrics 33
2.4.1 Failure Rate 34
2.4.2 Mean Time to Failure 36
2.4.3 Mean Time to Repair 37
2.4.4 Availability and Average Availability 37
2.4.5 Some other important metrics 38
2.5 State Space Model and Related Concepts 39
2.5.1 State Machines 39
2.5.2 Unified modeling Language (UML) 42
2.5.3 Markov Model 50
2.5.4 Petri Net 58
2.6 Conclusion 63

3 Reliability and Safety: State-of-the-art and Perspectives 65
3.1 Introduction 66
3.2 Reliability and Safety Concepts: 68
3.3 A Case Study 73
3.3.1 DFWCS Overview 74
3.3.2 Operating Modes 74
3.3.3 Physical Connections for the DFWCS 75
3.3.4 Possible Failures for the DFWCS 75
3.4 Reliability Prediction: State-of-the-art and Perspectives 77
3.4.1 Phase 1: Requirement analysis of the SCCS 78
3.4.2 Phase 2: Partitioning the SCCS into software components, interfaces, and hardware components 78
3.4.3 Phase 2.A: Software system analysis 78
3.4.4 Phase 2.A.1: Software system requirement analysis 80
3.4.5 Phase 2.A.2: Identification of critical software components . . 80
3.4.6 Phase 2.A.3: Development of reliability model for software system 80
3.4.7 Phase 2.A.4: Software system reliability prediction 81
3.4.8 Phase 2.A.5: Sensitivity analysis 81
3.4.9 Phase 2.A.6: Validation of analysis methodology 81

3.4.10 Phase 2.B and its sub phases: Reliability prediction for interfaces 82
3.4.11 Phase 2.C and its sub phases: Reliability prediction for hardware system 82
3.4.12 Phase 3: Overall reliability prediction for SCCS 82
3.4.13 Phase 4: Experimental Validation 83
3.5 Safety Prediction: State-of-the-art and Perspectives 123
3.6 Limitations of existing approaches 152
3.6.1 Modeling Limitations 152
3.6.2 Analysis Limitations 153
3.6.3 Parameter Estimation Limitations 154
3.6.4 Validation Limitations 154
3.6.5 Optimization Limitations 155
3.7 Conclusion 155

4 Problem Formulation and Solution Strategies 159
4.1 Introduction 160
4.2 Problem Formulation 163
4.2.1 Difficulty in generalization of the quantitative safety analysis methodology 163
4.2.2 Uncertainty in State-space models 165
4.3 Solution Strategies 165
4.3.1 Strategy for dealing with the difficulty in generalization of the quantitative safety analysis methodology 166
4.3.2 Strategy for dealing with the uncertainty in State-space safety models 167
4.4 Conclusion 168

5 A Probabilistic Hazard Assessment Framework for the Safety Critical and control System 169
5.1 Introduction 170
5.2 Related Work 171
5.3 The Proposed Method for Quantification of Hazards with a Case Study Illustration 174
5.3.1 Phase 1: Develop State Machine Model of the System 175
5.3.2 Phase 2: Identify Possible Failures from State Transition Diagram 176
5.3.3 Phase 3: Identify Possible Failures from State Transition Diagram 176
5.3.4 Phase 4: Map Failure Rate to All Identified Hazards Based on SIL (IEC 61508) 178
5.3.5 Phase 5: Expand State Machine with Failure Rate 179

5.3.6 Phase 6: Convert the State Machine into CTMC Model and Assessment of Hazard Probability . . . 181
5.4 Experimental Validation . . . 183
5.5 Conclusion . . . 187

6 Transformation of Deterministic Models into State space Models for Safety analysis of safety Critical Systems: A Case Study of Nuclear Power Plant 189
6.1 Introduction . . . 190
6.2 Related Work . . . 191
6.3 A Case Study . . . 194
6.3.1 RCICS Overview . . . 194
6.3.2 RCICS Operation and Operating Modes . . . 196
6.4 The Proposed Method For Safety Analysis By Use Of Conversion The UML Model into Petri Net Model with A Case Study Illustration . . 197
6.4.1 Phase 1: Requirements Analysis . . . 197
6.4.2 Phase 2: Identification of Possible Failures . . . 198
6.4.3 Phase 3: Formulation of USCD . . . 200
6.4.4 Phase 4: Validation of USCD . . . 201
6.4.5 Phase 5: Generation of PN Model from USCD . . . 201
6.4.6 Phase 6: Analysis Methodology Validation . . . 203
6.5 Conclusions . . . 212

7 Conclusion and Future Research 215
7.1 Difficulty in Generalizing the Quantitative Safety Analysis Methodology . . . 216
7.2 Uncertainty in State space Models . . . 217
7.3 Future Work . . . 218

Bibliography 219

A List of Publications 237

PREFACE

A safety-critical system executes the critical tasks, the failure of which may jeopardize human life, lead to considerable financial misfortune, or cause extensive environmental damage. Therefore, safety is considered as one of the most critical areas of research, while dealing with safety-critical systems. Traditional safety-critical systems are being converted into digital systems for several benefits. To support various features of a safety-critical system, the digital systems are becoming more complex in functional behaviors. Complex digital systems comprised of many software and hardware components mostly of them are heterogeneous in nature. A safety-critical system comprises of a large no. of heterogeneous components, there is higher risk always associated with the safety-critical systems due to possible failures in Hardware/Software involved there in. Several techniques are available to perform the safety analysis of such systems. An extensive literature survey was carried out to identify the available methods for safety analysis of safety-critical digital systems. Most of them works on qualitative assessment rather than quantitative assessment. However, quantitative assessment has several benefits over qualitative assessment such as – (i) risks are sorted by their adversity impact, and (ii) security levels can be better determined/defined through consideration of three elements that are availability, integrity, and confidentiality. Further, safety analysis during the early phases of system development life cycle has many significant benefits such as – (i) help in taking decisions to select most suitable design (ii) cost minimization (iii) analyzing the sensitivity of the system safety to its component safety (iv)identify safety bottlenecks. The proposed work deals with a new probabilistic approach to quantify safety of safety-critical systems during the design phase of the systems that is based on the probabilistic safety assessment to deal with the shortcomings of the existing techniques using state-space models.

Further, it is a challenging task to capture all the requirements including safety requirements through state space models. Also, verifying that the constructed model has captured all the requirements is again a problem in itself, because of all the understanding of stakeholders may not get captured during development of the state-space model. Failing to model all the requirements will give inaccurate safety assessment. UML is a well-known and successful way of modelling which is used for specifying requirements. UML can capture all the requirements and be easily understood by all the stakeholders. This motivates us to propose a methodology to convert the UML model into a state space model that can be used for quantitative assessment of a safety-critical systems under consideration. A framework is proposed and introduced in this thesis to transform UML model into a state-space model in the form of a Petri net, which is a reliable graphical and mathematical tool to perform several static and dynamic analysis.

All the above proposed approaches are validated considering a real-time safety-critical system of Nuclear Power Plant along with some noticeable findings.